

the pending claims is amended to recite analyzing security information *that is* collected from a user contemporaneously with the initiation of a *process control* function implemented within a process control system and wherein the execution of the *process control* function is determined based on the contemporaneously collected security information. This amendment serves only to clarify (to the extent the claims were not already clear) that the collection of security information is performed contemporaneously with the initiation of the process control function, and not, as previously interpreted by the Office, as analyzing security information contemporaneously with the initiation of the function.

Because He et al. fails to disclose the collection of security information from a user contemporaneously with the initiation of a process control function to determine whether the process control function may be executed, He et al. cannot anticipate any of the pending claims. Generally speaking, He et al. discloses an authentication process where a security server issues a session ticket to a user machine which subsequently requires a valid user login and password before the session ticket can be used. Thereafter, any subsequent communication between the user machine and the server or other network element requires passing the stored session ticket without further authentication input from any user. In fact, He et al. specifically states that

“[t]he NSS 208 [the security server]... generates a general ticket to be used by the user element for future network access requests. After ID and password authentication has been completed, the general ticket is encrypted using a secret key assigned by, and only know[n] to, the NSS 208 so that future access requests by the same user element can be quickly authenticated by the NSS 208. **This avoids the NSS 208 having to verify the ID and password each time the user element makes an access request.**” Col. 27 lines 23-31 (emphasis added).

Thus, after the first time the user logs on to a particular user machine within the He et al. system (it being understood that such a log on procedure is not the initiation of a process

control function), the user machine may be used to access a server or network element without any further collection of security information from the user. Thus, He et al. does not disclose the collection of security information from the user contemporaneously with the initiation of a process control function for determining whether the process control function may be executed, as recited by the pending claims. Instead, He et al. only discloses using previously collected (and stored) security information upon the initiation of a function, similar to other known systems.

Moreover, as discussed in the interview, column 9, lines 47-61 of the He et al. patent fails to disclose collecting security information from a user contemporaneously with the initiation of a function. While column 9, lines 47-61, of He et al. states that “[u]ser access authorization and control must be performed for each and every individual user request to access network resources and information,” this passage does not indicate or even suggest that the system should collect user security information for each user request at the time that a process control function is initiated. In fact, He et al. (at least at col. 17, line 28 – col. 22, line 23; Fig. 6; and Col. 27, lines 23-39) describes with a high degree of particularity that its user access authorization involves the issuance and transmission of a previously stored session ticket, not the collection of security information from a user at the time the user makes a function request.

As a result, the He et al. system, similar to other known systems, contains a security loophole. In particular, after a user logs on to a user terminal, thereby completing the general system authentication procedure, any other person may use that same user terminal to access process control functions enabled by the login procedure. The system and method of the pending claims, on the other hand, prevent unauthorized execution of, for example, critical process control functions by requiring collection of security information from the user

contemporaneously with the initiation of a process control function and using the contemporaneously collected security information to determine whether the process control function may be executed. For these reasons, He et al. cannot anticipate any of the pending claims.

Furthermore, it is clear that the prior art must make a suggestion of or provide an incentive for a claimed combination of elements to establish a *prima facie* case of obviousness. See, *In re Oetiker*, 24 U.S.P.Q.2d 1443, 1446 (Fed. Cir. 1992); *Ex parte Clapp*, 227 U.S.P.Q. 972, 973 (Bd. Pat. App. 1985). This principle holds true even if the applied art could be modified to produce the invention recited by the pending claims. See, *In re Mills*, 16 U.S.P.Q.2d 1430, 1432 (Fed. Cir. 1990); *In re Gordon*, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984) ("The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification.") Because He et al. fails to disclose or provide any motivation for collecting security information from a user contemporaneously with the initiation of a process control function within a process control system, it follows that He et al. cannot render any of the claims at issue obvious.

Applicants note that the amendments to the claims are made herein solely to protect the claims against any possibility of grammatical ambiguity. The amendments do not alter the scope of the original claims and thus, do not and cannot raise new issues. As a result, the amendments should be entered. Furthermore, Applicants note that MPEP Section 904 specifically states that "[t]he first search [of prior art] should cover the invention as described and claimed, including the inventive concepts toward which the claims appear to be directed. **It should not be extended merely to add immaterial variants.**" (emphasis added) MPEP § 904. Since the amendments to the claims are merely grammar refinements which do not alter

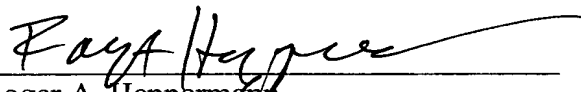
claim scope, no new search is required at this time. In fact, as evidenced in each Office Action Response filed to date, Applicants have asserted a consistent interpretation of the claims that is supported by the grammar of the original claims and only bolstered by the current amendment. Because the Office has been or should have been aware of the Applicants' asserted claim scope from the original specification as well as from each Office Action Response, a new search at this time would only serve to place undue hardship on the Applicants, in the form of requiring the Applicants to pay additional fees and in delaying issuance of a patent, without any benefit to the Office. Because the grammatical refinements included by this amendment cannot possibly affect the search originally performed by the Office in fulfilling its examination duties, Applicants submit that, in accordance with MPEP § 904, no new issues have been raised. Therefore, conducting an extended search for the immaterial claim changes hereby is not necessary.

**CONCLUSION**

For the foregoing reasons, Applicants respectfully request entry of this amendment, reconsideration and withdrawal of the rejections, and allowance of claims 1-18, 20-29, and 32. If there are matters that can be discussed by telephone to further the prosecution of this application, Applicants respectfully request that the Examiner call its attorney at the number listed below.

Respectfully submitted,

By:

  
\_\_\_\_\_  
Roger A. Heppermann  
Registration No. 37,641  
Attorney for Applicants

MARSHALL, GERSTEIN & BORUN LLP  
6300 Sears Tower  
233 South Wacker Drive  
Chicago, Illinois 60606  
312-474-6300

**November 23, 2005**